Персональные данные в Облачных технологиях

+7 (495) 909 03 64 / www.iicavers.ru

Особенности нормативно-правовых актов Российской Федерации в области защиты персональных данных

8 ноября 2001 года

Конвенция **ETS N 108** подписана от имени Российской Федерации

19 декабря 2005 г.

Федеральный закон N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных"

27 июля 2006 г.

Федеральный закон N 149-ФЗ « Об информации, информационных технологиях и о защите информации"

Федеральный закон N 152-ФЗ « О персональных данных"

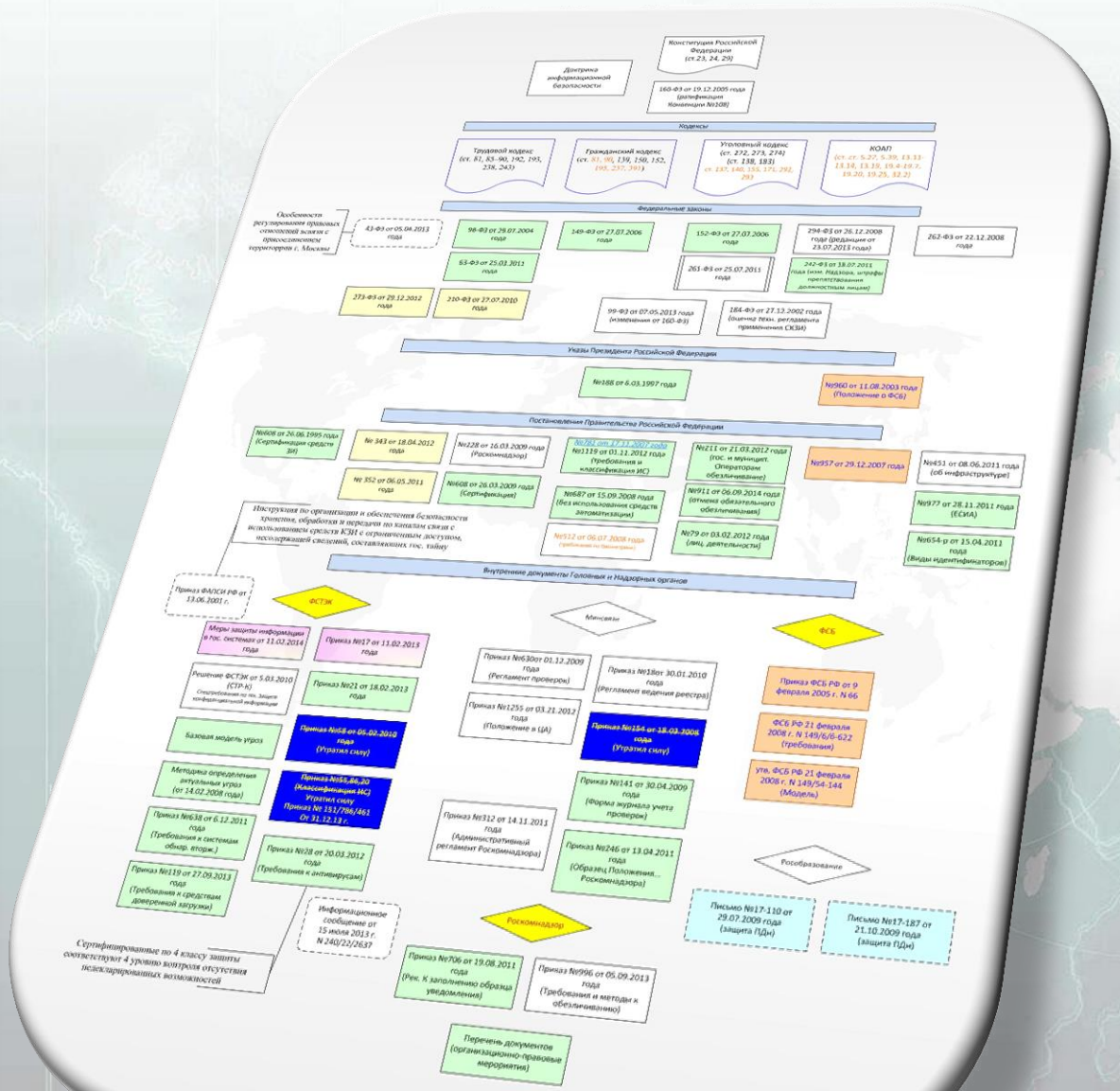
21 мая 2013 г.

Сообщение МИД России «О вступлении в силу для РФ Конвенции о защите физических лиц при автоматизированной обработке персональных данных»

1 сентября 2013 г.

Правовое поле

*"Можно быть уверенным только в двух вещах: существовании вселенной и человеческой глупости и я не совсем уверен насчет первой" – **Л. Эйнштейн**.*



ФСБ России

ФСТЭК России

Роскомнадзор

ФЕДЕРАЛЬНЫЙ ЗАКОН № 152 ОТ 27 ИЮЛЯ 2006 Г.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

- персональные данные
- специальные категории персональных данных
- биометрические персональные данные

- Конфиденциальность
- Целостность
- Доступность

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Постановление Правительства РФ от 1 ноября 2012 г. **№1119** "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Постановление Правительства РФ от 15 сентября 2008 г. **№687** "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"

Постановление Правительства РФ от 06.07.2008 года **№512** "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"

РОСКОМНАДЗОР

Требования, предъявляемые к операторам, осуществляющим обработку персональных данных

Уведомление об обработке персональных данных

Согласие субъекта персональных данных на обработку его персональных данных в письменной или иной форме

Организационно-распорядительные документы по соблюдению требований законодательства

Документы подтверждающие уничтожение Оператором персональных данных субъектов персональных данных по достижении цели обработки

Локальные акты Оператора, определяющие его политику в отношении обработки персональных данных и устанавливающие требования и процедуры по предотвращению и выявлению нарушений, устранению их последствий

Соблюдение установленного порядка и условий обработки персональных данных в информационных системах персональных данных.

37 – 45

Алгоритм построения информационных систем ПДн. Что должен знать руководитель?

Постановление №1119 от 1 ноября 2012 г.

Порядок проведения классификации информационных систем персональных данных

ФСТЭК России

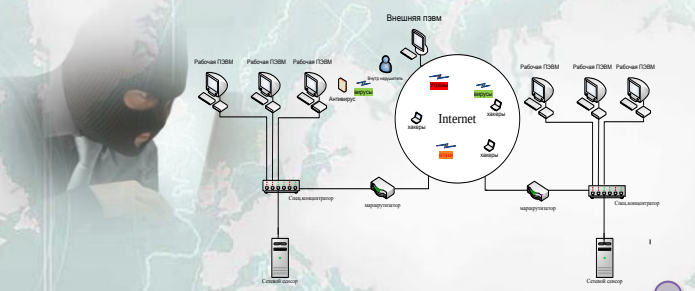
Методика определения актуальных угроз

Базовая модель угроз

Приказ №21 от 18.02.2013 года

Приказ № 28 от 20.03.2012 года

Приказ № 638 от 06.12.2011 года



Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИС ПДн

Требованиям к средствам антивирусной защиты

Требованиям к системам обнаружения вторжений

ФСБ России

СКЗИ

Приказ N 66 от 9 февраля 2005 г.

Требования N 149/54-144 от 21 февраля 2008 г.

Требования N 149/6/6-622 от 21 февраля 2008 г.

Роскомнадзор

Перечень документов (организационно-правовые меры)

Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью **системы защиты персональных данных**, нейтрализующей актуальные угрозы

1-го типа

2-го типа

3-го типа

Актуальные угрозы безопасности

Уровень защищенности персональных данных

1-й уровень | 2-й уровень | 3-й уровень | 4-й уровень

Модель угроз

Модель нарушителя

Базовая модель угроз

Методика определения угроз

N 149/54-144
от 21 февраля 2008 г.

Организационные меры

Технические меры

4-й уровень

Режим обеспечения безопасности помещений

Сохранность носителей персональных данных

Перечень лиц, допущенных к ПДн обрабатываемым в ИС

СЗИ прошедшие процедуру оценки соответствия

3-й уровень

Должностное лицо (работник), **ответственный** за обеспечение безопасности ПДн в ИС

2-й уровень

Ограничение доступа к содержанию электронного журнала сообщений

1-й уровень

Автоматическая регистрация изменения полномочий по доступу к ПДн в ИС

Структурное подразделение, ответственное за обеспечение безопасности ПДн в ИС

Защита персональных данных в облачных технологиях. Кто несет ответственность?

ЦОД

*Центр (хранения и) обработки данных **(ЦОД/ЦХОД)** — это специализированное здание для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет.*

SaaS

Software as a service

программное обеспечение как услуга

Полный доступ

Paas

Platform as a Service

платформа как услуга

Администрирование и управление

IaaS

Infrastructure-as-a-Service

инфраструктура как услуга

Физический доступ

*С момента появления в 2006 году концепция глубоко проникает в различные информационно-технологические сферы и занимает всё более и более весомую роль в практике: по оценке IDC **рынок** публичных **облачных вычислений** уже к 2009 году составил $17 млрд — около **5 %** от всего рынка информационных технологий, а в **2014** году суммарные затраты организаций на инфраструктуру и услуги, связанные с облачными вычислениями, оцениваются почти в **$175 млрд**.*

Как правило, взаимоотношения **ЦОД – Оператор** характеризуются Договором оказания услуг (~~Договор обработки персональных данных~~)

РОСКОМНАДЗОР

Административный штраф

«Облако»

ЦОД – третье лицо

Обработка ПДн

Оператор

Субъект ПДн

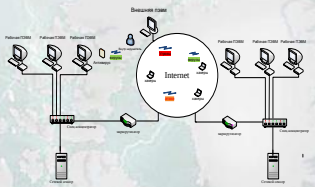
п. 5 ст.6 152-ФЗ

IaaS

Paas

SaaS

Возможно привлечение ЦОД к договорной ответственности за несоблюдение условий договора о гарантиях физической безопасности информации



ИС ПДн

п.3 ст. 6 152-ФЗ

Задача – **создание ИС**, обеспечивающей обработку и хранение ПДн, полученных Оператором.

Договор об обработке и хранении ПДн может быть заключен в виде договора оказания услуг или договора поручения.

Необходимые Положения для включения в договор:

1. **Перечень действий** (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн
2. **Цели и порядок** обработки хранения и уничтожения ПДн
3. **Обязанность** третьего лица соблюдать **конфиденциальность** ПДн и безопасность ПДн при их обработке
4. Требования к **защите** ПДн (ст.19 152-ФЗ)

Лестница в 7 ШАГОВ

1. Определение вида услуг оказываемых ЦОД: **SaaS, PaaS, IaaS**
2. Классификация ИС ПДн
3. Совместное моделирование угроз
4. Выработка организационных и технических мер
5. Подготовка организационно-распорядительных документов
6. Получение согласия СПДн о передаче обработки ПДн третьему лицу
7. Юридическое оформление взаимоотношений: **Оператор – ЦОД** (заключение договоров и подготовка организационной документации взаимодействия)

Делегирование Ответственности
Оператор - ЦОД

Оказание услуг по размещению информации на серверах ЦОД («Облачных сервисах»)

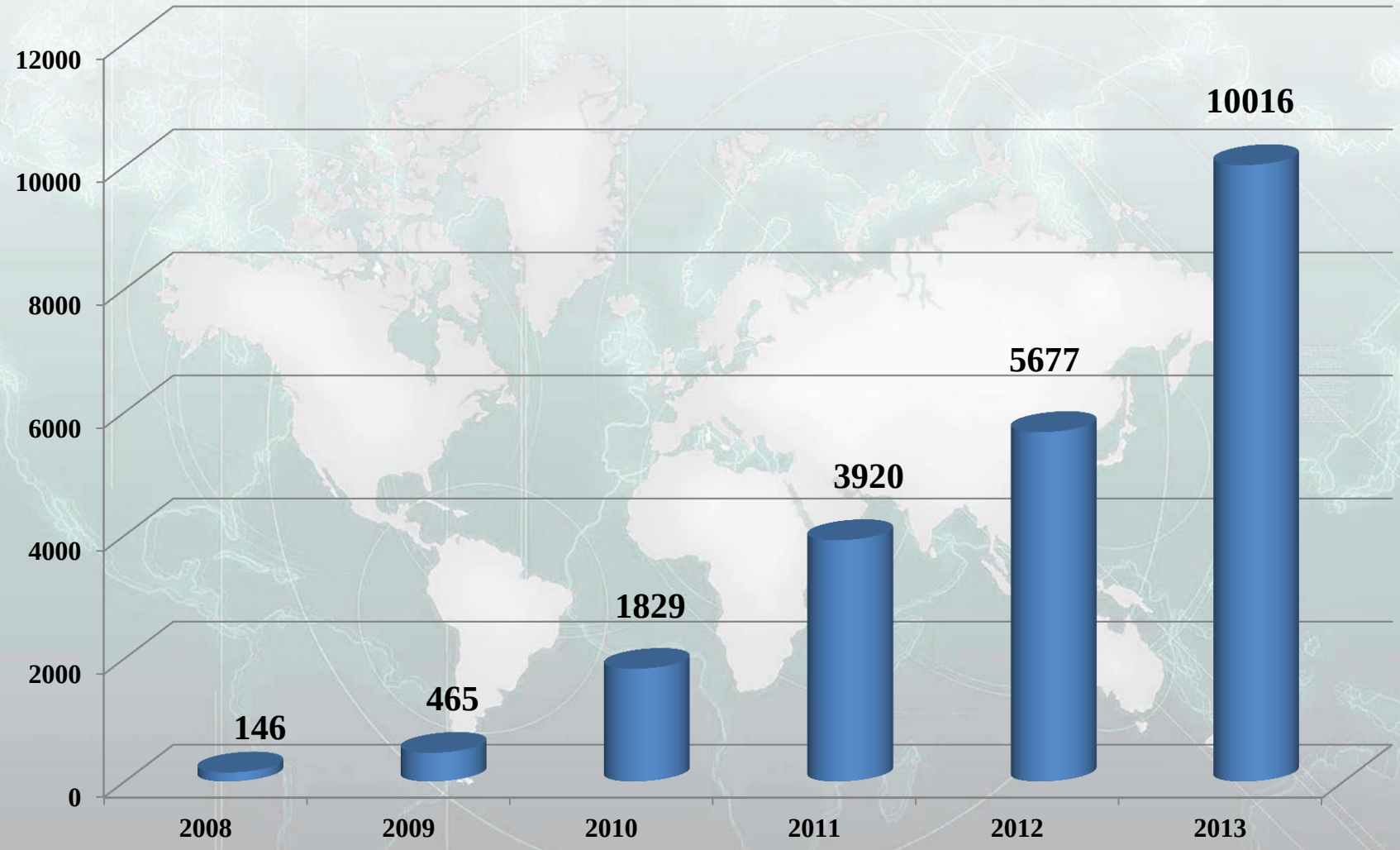
На обработку, хранение и уничтожение ПДн (обязательно включение Целей и задач обработки)

Нейтрализация угроз

Порядок получения, обработки, хранения и уничтожения ПДн

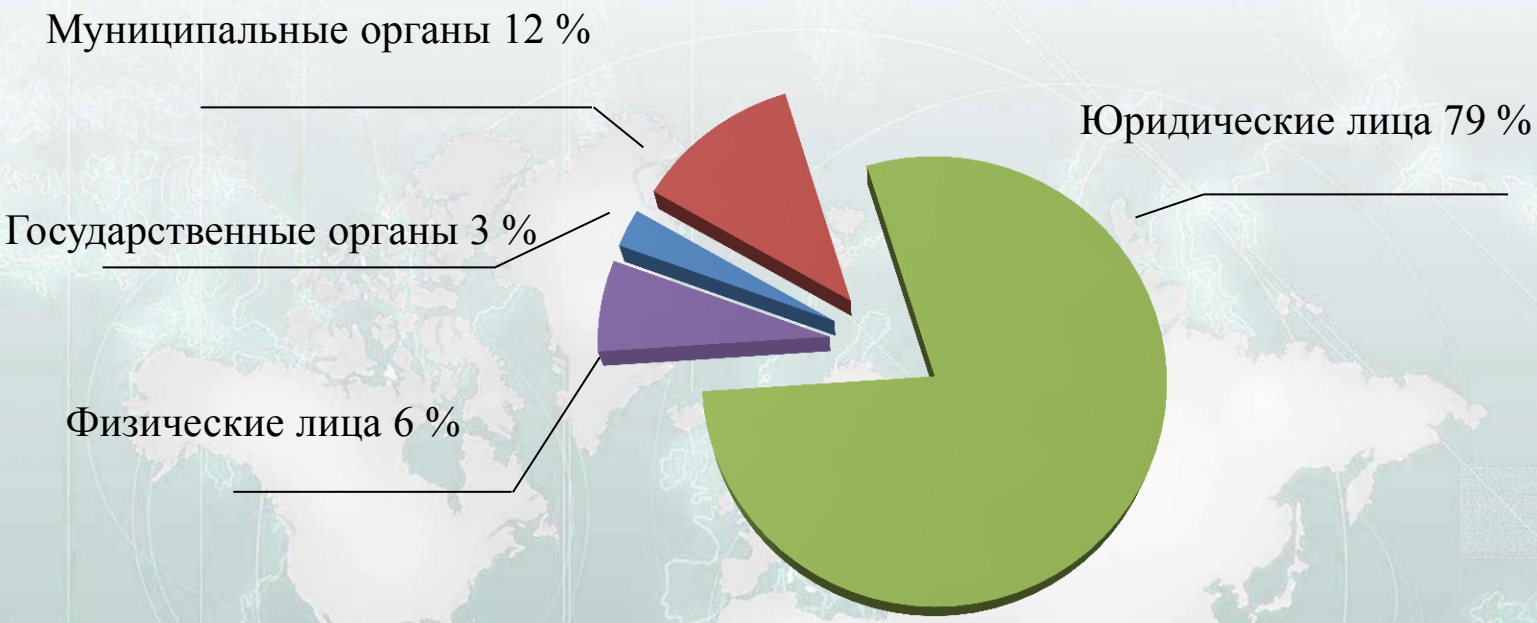
Порядок возмещения убытков

Обращения граждан и юридических лиц



РОСКОМНАДЗОР

Из общего числа Операторов, внесенных в Реестр:



общеобразовательные школы – 36 414
дошкольные учреждения – 32 022
учреждения здравоохранения и социального обеспечения – 12 375
учреждения ЖКХ (ТСЖ) – 8 572
средние и высшие учебные заведения профессионального образования – 2 355
кредитные учреждения – 1 546
туроператоры – 513
коллекторские агентства – 138

Спасибо за внимание !

Обращайтесь к нам:

Группа компаний «Аверс»

office@iicavers.ru

Согласно части 4 ст. 1255 Гражданского кодекса РФ от 18.12.2006 года N 230-ФЗ

При подготовке презентации использовались материалы информационных ресурсов:

http://government.ru	**http://fsb.ru**
http://www.garant.ru	http://fstec.ru
http://www.itsec.ru	http://rkn.gov.ru